CLAIMS

Bully 1

[]]

in the second

2

6

An X.509 certificate capable of supporting more than one cryptographic algorithm, comprising:

a signature algorithm and signature for all authenticated attributes using a first cryptographic

3 algorithm;

an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

- 2. An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.
- 3. An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

CR9-98-09